# TTP Detail – T1003.006

## TTP Information

Name: DCSync

Description: Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (API)(Citation: Microsoft DRSR Dec 2017) (Citation: Microsoft GetNCCChanges) (Citation: Samba DRSUAPI) (Citation: Wine API samlib.dll) to simulate the replication process from a remote domain controller using a technique called DCSync.

Members of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts on the domain controller are able to run DCSync to pull password data(Citation: ADSecurity Mimikatz DCSync) from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) for use in [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003)(Citation: Harmj0y Mimikatz and DCSync) or change an account's password as noted in [Account Manipulation](https://attack.mitre.org/techniques/T1098).(Citation: InsiderThreat ChangeNTLM July 2017)

DCSync functionality has been included in the "lsadump" module in [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: GitHub Mimikatz lsadump Module) Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol.(Citation: Microsoft NRPC Dec 2017)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* Mimikatz

## APTs (Intrusion Sets)

* Earth Lusca
* LAPSUS$